КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.25.200214
УДК 004.056.2

Чура Тарас Русланович
аспірант кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка», Львів, Україна
ORCID ID: 0009-0001-1898-9879
taras.r.chura@lpnu.ua

Чура Назар Русланович
аспірант кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка», Львів, Україна
ORCID ID: 0009-0006-9072-0045
nazar.r.chura@lpnu.ua

ОГЛЯД СУЧАСНИХ МЕТОДІВ АВТЕНТИФІКАЦІЇ ДЛЯ МІКРОКОНТРОЛЕРІВ

Анотація. Робота присвячена дослідженню сучасних методів автентифікації мікроконтролерів, які займають важливе місце в сучасному технологічному ландшафті. Мікроконтролери є основою більшості вбудованих пристроїв, що використовуються в різних сферах, включаючи побутову електроніку, автомобільні системи, промислове обладнання та медичні пристрої. Вони виконують ключові функції, пов'язані з управлінням, контролем і моніторингом безлічі процесів та систем. З огляду на широке впровадження мікроконтролерів у критично важливі інфраструктури, питання забезпечення їхньої безпеки стає пріоритетним. Автентифікація мікроконтролерів має вирішальне значення для захисту від несанкціонованого доступу та кібератак, що можуть призвести до серйозних наслідків, зокрема втрата даних, контроль над системами або збої в роботі критичних сервісів. У роботі детально розглядається значущість безпеки мікроконтролерів у сучасних технологіях та досліджуються потенційні ризики, що виникають внаслідок використання незахищених мікроконтролерів. Також у роботі проаналізовано сучасні методи автентифікації, що використовуються для захисту мікроконтролерів. Особливу увагу приділено порівнянню різних підходів до автентифікації, що включає як традиційні, так і нові методи, що ґрунтуються на криптографії, фізичних неклонованих функціях (PUF) та біометрії. Для кожного з методів наведено їхні переваги, недоліки та сфери застосування, а також оцінено їхню ефективність у контексті різних сценаріїв безпеки. Крім того, в роботі описано результати практичного застосування деяких методів автентифікації на реальних прикладах, що підтверджують їхню життєздатність і ефективність у захисті сучасних систем. Автори також пропонують майбутні напрямки досліджень у цій сфері, зокрема розробку нових методів автентифікації, що поєднують високу надійність і простоту впровадження в умовах швидкого розвитку технологій та кіберзагроз.

Ключові слова: кібербезпека; вразливості; безпека мікроконтролерів; методи автентифікації.

ВСТУП

Постановка проблеми. У сучасному світі мікроконтролери стали невід'ємною складовою багатьох технологічних рішень. Вони використовуються в різноманітних пристроях, починаючи від домашніх електронних пристроїв і закінчуючи автомобільними системами управління. За допомогою мікроконтролерів реалізується автоматизація, контроль і моніторинг, що підвищує ефективність та зручність використання техніки. Однак, разом з поширенням використання мікроконтролерів, зростають і потенційні загрози, пов'язані з їхньою безпекою.

Мікроконтролери використовуються у різних сферах життя, і кожна з них має свої особливості та вимоги щодо безпеки. У промисловості мікроконтролери дозволяють автоматизувати виробничі процеси та контролювати роботу обладнання. Проте, вразливість мікроконтролерів може призвести до великих збитків через зловживання з боку зловмисників. Тому забезпечення безпеки в промислових системах, де використовуються мікроконтролери, має велике значення для попередження можливих кібератак.

У медичній сфері мікроконтролери використовуються для розробки медичних приладів та систем моніторингу, які збирають та аналізують дані про стан здоров'я пацієнтів. Забезпечення цих систем безпекою є критично важливим, оскільки будь-яка помилка чи порушення може призвести до серйозних наслідків для здоров'я пацієнтів.

У сфері автомобільної техніки мікроконтролери використовуються для управління різними системами автомобіля, такими як системи безпеки, навігації, комфорту та розваг. Вразливість мікроконтролерів у таких системах може призвести до небезпечних ситуацій на дорозі та загрози життю водіїв та пасажирів.

У побутових пристроях, таких які використовуються у розумних домах, мікроконтролери використовуються для автоматизації різних функцій, таких як управління освітленням, опаленням та безпекою. У разі порушення безпеки цих систем може виникнути загроза приватності та безпеки мешканців будинку. Отже, підвищення безпеки мікроконтролерів має велике значення для забезпечення стабільності та безпеки різних систем, що використовують ці пристрої.

В цій статті буде зроблений огляд сучасної літератури на тему способів і методів підвищення безпеки мікроконтролерів, щоб оцінити стан безпеки на сьогоднішній день, з'ясувати чи є універсальний метод, який би підійшов для всіх без винятку мікроконтролерів та подивитись на майбутні способи покращення.

Заходи безпеки можуть включати в себе розробку захисту від вразливостей, шифрування комунікацій, перевірку програмного забезпечення на вразливості та впровадження механізмів виявлення та відновлення у разі атак. Крім того, важливо проводити регулярні аудити безпеки та надавати користувачам можливість оновлення пристроїв для виправлення виявлених вразливостей.

У світі, де технології стають все більш інтегрованими у наше повсякденне життя, безпека мікроконтролерів є ключовим аспектом для забезпечення стабільності, надійності та безпеки різних систем. Розвиток технологій безпеки мікроконтролерів є важливим завданням для індустрії та суспільства в цілому, і лише за умови його вирішення ми зможемо максимально використовувати потенціал цих пристроїв у сучасному світі.

Аналіз останніх досліджень та публікацій. За останні 100 років кількість згадок про мікроконтролери у науково-технічній літературі безперервно зростає по всьому світу, це ілюструють дані, наведені на рис. 1, рис. 2, рис. 3.Тематика мікроконтролерів приваблює не тільки дослідників розробників систем безпеки, але і зловмисників, які змагаються в парадигмі «меча і щита».

ISSN 2663 - 4023

Графіки кількості згадок поняття «мікроконтролер» в літературі за останні 100 років

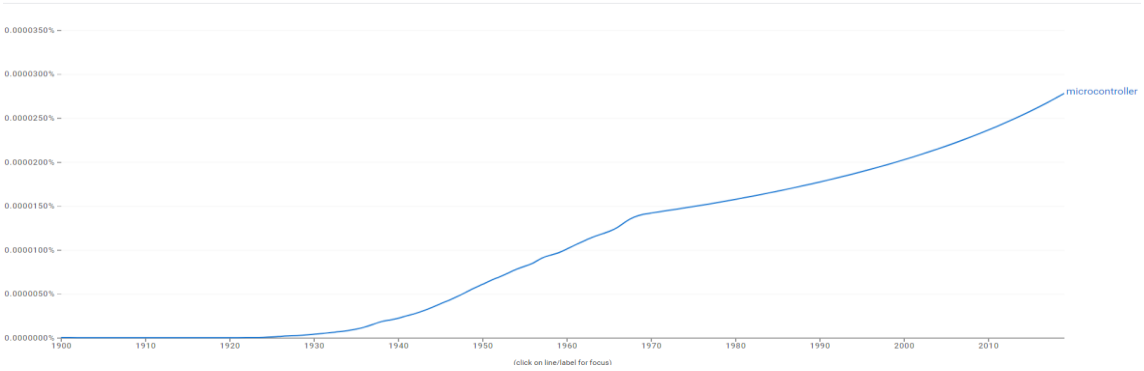

Рис. 1. Кількість згадок поняття «мікроконтролер» в британській літературі

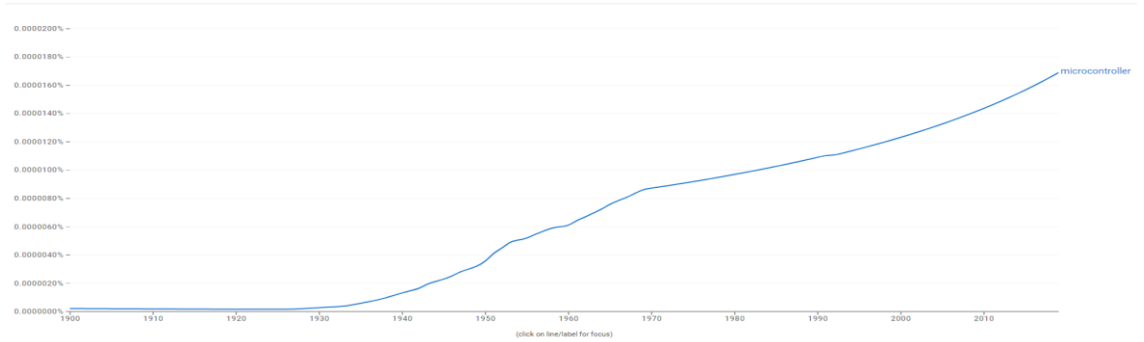

Рис. 2. Кількість згадок поняття «мікроконтролер» в американській літературі

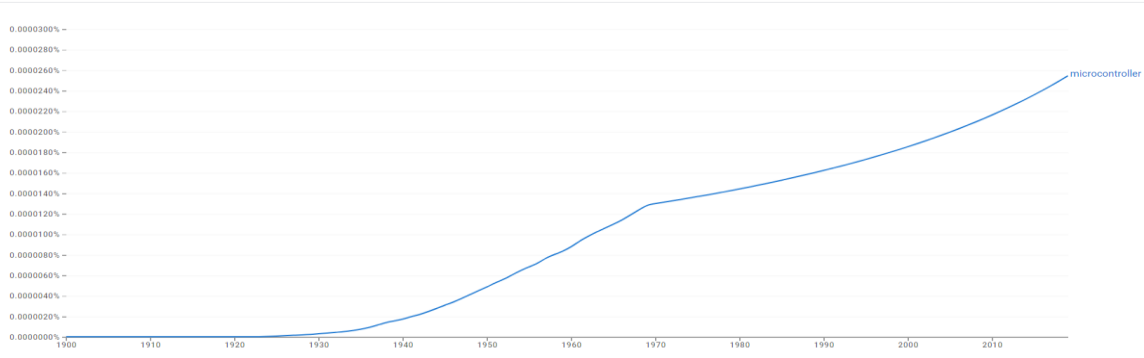

Рис.3. Кількість згадок поняття «мікроконтролер» в літературі англійською мовою в решті світу

Далі розкажемо про найцікавіші опрацьовані статті за темою безпеки мікроконтролерів, щоб розібратись із методами їх автентифікації, опишемо переваги та недоліки кожного методу та покажемо загальну порівняльну таблицю по можливих атаках на системи автентифікації цими методами.

В 2015 році була представлена нова архітектура — Secure Execution PUF-based Processor (SEPP), що призначена для вирішення проблем безпеки під час виконання програм [1]. Вона використовує фізично не клоновані функції (ФНФ) і шифрування коду на рівні інструкцій для захисту від атак із впровадженням коду та збереження

конфіденційності коду. Архітектура SEPP мінімізує сфери можливих атак та вплив на продуктивність, не вимагаючи значних змін у процесі розробки. Вона інтегрує ФНФ безпосередньо в конвеєр інструкцій процесора, підтримуючи безпечні середовища віддаленого виконання.

Системи боротьби з підробкою на основі міток радіочастотної автентифікації (RFID), зосередженим на різних методах боротьби з підробкою в різних галузях промисловості детально розглянуто у [2]. Автори описали впровадження технології RFID, включаючи не клоновані мікросхеми RFID на основі ФНФ, мітки RFID без мікросхем, системи відстеження, протоколи обмеження відстані та криптографічні методи.

Також в 2019 році представлено «DRAMNet», інноваційний метод автентифікації, який використовує унікальні функції послідовностей активації DRAM, використовуючи глибокі згорткові нейронні мережі (ЗНМ) для забезпечення контролю доступу, особливо в автономних транспортних засобах і дронах [3]. Він перетворює послідовність увімкнення DRAM у 2D-зображення, щоб отримати характерні особливості для автентифікації пристрою, досягаючи високої точності. DRAMNet представляє новий підхід до поєднання фізичних характеристик апаратного забезпечення з машинним навчанням для підвищення безпеки, підкреслюючи його потенціал у різних програмах, одночасно розглядаючи майбутні вдосконалення та ширші сценарії тестування.

Також в 2019 році було оглянути методи безпеки та точності біометричних систем на основі відбитків пальців [4]. Автори описали різні атаки на ці системи, заходи протидії цим загрозам і важливість досягнення високої точності розпізнавання. У документі наголошується на поточних проблемах, пов’язаних із забезпеченням балансу між безпекою та продуктивністю розпізнавання, підкреслюючи необхідність подальших досліджень щодо покращення надійності та надійності біометричних систем автентифікації.

В 2020 році було представлено ФНФ як апаратне рішення для підвищення безпеки IoT. ФНФ використовують унікальні фізичні характеристики пристроїв для безпечної ідентифікації та автентифікації, пропонуючи практичний підхід для генерації секретних ключів [5].

Також в 2020 році представлено концепцію оптичної ідентифікації (OI) для підвищення безпеки мережі на фізичному рівні, використовуючи унікальні властивості ФНФ [6]. Ця ідентифікація зоснована на використанні зворотного розсіювання Релея як оптичного ФНФ для безпечної ідентифікації та автентифікації різних компонентів у системах і мережах оптичного зв’язку. Цей метод дозволяє ідентифікувати мережеві підсистеми на фізичному рівні без додаткових пристроїв, маючи тим самим потенціал для значного підвищення безпеки за допомогою автентифікації та моніторингу оптичних мереж і систем.

В 2021 зроблено огляд простих алгоритмів криптографії для мереж Інтернету речей (IoT), які вирішують унікальні проблеми безпеки, з якими стикаються пристрої IoT через їх обмежену пам’ять та обчислювальну потужність [7]. В дослідженні описано різні криптографічні технології, тенденції та конкретні вимоги до безпеки IoT, включаючи порівняння існуючих рішень. Акцент робиться на придатності легких симетричних шифрів для пристроїв IoT для забезпечення конфіденційності, цілісності та автентичності даних з мінімальним споживанням ресурсів.

В 2022 році було досліджено використання легких протоколів автентифікації для пристроїв Інтернету речей (IoT), зосереджених на їх придатності для середовищ з обмеженими ресурсами [8]. Було досліджено різні протоколи на основі використання

пам’яті, затримок, пропускної здатності та споживання енергії, забезпечуючи рейтинг продуктивності для кожного показника. Дослідження підкреслює важливість вибору правильного протоколу на основі конкретних вимог програми IoT, включаючи вартість і продуктивність.

В цьому ж році був опублікований огляд сучасних методів автентифікації, в якому розглядаються процеси однофакторної, двох факторної та багатофакторної автентифікації та їхні критерії [9]. Він оцінює різні методи автентифікації, включаючи безпеку пароля, біометричні дані та методи веб-автентифікації, а також розглядає проблеми та майбутні напрямки розвитку MFA. Дослідження підкреслює важливість вдосконалення механізмів автентифікації для захисту систем від несанкціонованого доступу, припускаючи, що, незважаючи на прогрес, прості паролі залишаються широко використовуваними, тоді як MFA пропонує вищий рівень безпеки.

Також в 2022 році описано легкий і практичний протокол анонімної автентифікації на основі ФНФ бітового самотестування (BST-PUF) [10]. Він вирішує проблеми безпечного зв’язку в малоресурсних пристроях, представляючи новий алгоритм допоміжних даних (HDA), який уникає складних механізмів виправлення помилок, значно зменшуючи складність реалізації та накладні витрати на виконання. Цей протокол автентифікації покращує безпеку, запобігаючи відстеженню пристрою та витоку CRP, підтримуючи безпечну взаємну автентифікацію між пристроями та серверами без зберігання великих пар виклик-відповідь, тим самим захищаючи конфіденційність пристрою та зменшуючи потреби в сховищі на сервері.

В 2023 році обговорюється важливість створення унікальних і захищених від втручання ідентифікаторів для напівпровідникових компонентів, підкреслюючи їх роль у відстежуваності в ланцюжку постачання [11]. Досліджено різні технології для генерації унікальних ідентифікаторів, таких як оптичні ідентифікатори та ідентифікатори електронних чіпів (ECID), і описано використання ФНФ для створення безпечних ідентифікаторів пристрою. Ці технології мають вирішальне значення для вдосконалення виробничих процесів, забезпечення безпеки комп’ютерних додатків і запобігання контрафактній продукції в таких секторах, як автомобільна промисловість і медичне обладнання.

Також в 2023 році було досліджено використання даних акселерометра та гіроскопа зі смартфонів для ідентифікації та автентифікації користувачів [12]. Описано використання алгоритмів машинного та глибокого навчання для аналізу даних давачів з метою підвищення безпеки та конфіденційності. Дослідження оцінює різні методи вибору функцій і попередньої обробки для покращення продуктивності ідентифікації, порівнюючи дані акселерометра з даними гіроскопа для ефективності автентифікації.

В 2024 році представлено новий метод автентифікації на основі ФНФ і протокол обміну ключами для пристроїв IoT, які використовують легкі операції та працюють без необхідності активного підключення до Інтернету для пристрою IoT для захисту від атак [13]. Метод використовує побітове XOR, хеш-функції та ФНФ, придатні для середовища з обмеженими ресурсами.

Також в 2024 році представлено інноваційний підхід до розпізнавання ідентифікаторів пристроїв на основі адаптивних середовищ для відбитків пальців [14]. Підхід спрямований на підвищення точності розпізнавання відбитків пальців пристрою шляхом вирішення проблем, пов’язаних із змінами шуму навколишнього середовища. Дослідження представляє метод, який фіксує дані в режимі реального часу про вихідні параметри пристрою в зашумленому середовищі та використовує агреговану архітектуру нейронної мережі гіперграфа для обробки фізичних функцій, що змінюються в часі. Цей

метод значно підвищує надійність розпізнавання відбитків пальців пристрою на відкритому повітрі, досягаючи точності розпізнавання 98% у змінних умовах навколишнього середовища, тим самим підвищуючи безпеку пристроїв IoT відповідно до реальних викликів.

Мета статті. Метою статті є аналіз переваг і недолікив сучасних методів автентифікації мікроконтролерів

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

В цьому розділі буде описано переваги і недоліки методів автентифікації, які були опрацьовані в уже виданих статтях за цією тематикою. В кінці розділу буде подана порівняльна таблиця для розглянух методів по відношенню їх можливих вразливостей до популярних атак.

Фізично не клоновані функції

Автентифікація з використанням ФНФ — це метод, який використовується для захисту мікроконтролерів та інших вбудованих систем. ФНФ — це апаратні примітиви безпеки, які використовують фізичні відмінності, властиві напівпровідниковим пристроям, для створення унікальних ідентифікаторів або криптографічних ключів. Ці фізичні зміни виникають під час виробничого процесу, і їх практично неможливо відтворити, що робить ФНФ стійкими до атак клонування, від чого вони і отримали свою назву.

Переваги:

1. ФНФ використовують мінливість фізичних характеристик для створення унікальних ідентифікаторів або ключів для кожного пристрою. Цю унікальність можна використовувати для автентифікації пристрою, створення безпечних ключів та інших програм безпеки.
2. Теоретично ФНФ стійкі до спроб клонування, оскільки вони залежать від неконтрольованих змін фізичних властивостей. Навіть якщо зловмисник отримає доступ до пристрою, він не зможе просто скопіювати ключ на основі ФНФ.
3. На відміну від традиційних криптографічних ключів, які зберігаються в пам’яті, ФНФ генерують ключі на льоту з фізичних властивостей. Це позбавляє від необхідності зберігати їх в пам’яті, зменшуючи ризик їхнього розкриття.
4. ФНФ часто вимагають мінімальних обчислювальних ресурсів і потужності, що робить їх придатними для пристроїв з обмеженими ресурсами, таких як пристрої Інтернету речей і вбудовані системи.
5. ФНФ реалізовано в апаратному забезпеченні, що робить його стійким до програмних атак і шкідливих програм. Це додає системі додатковий рівень безпеки.

Недоліки:

1. ФНФ залежать від фізичних властивостей, на які можуть впливати фактори навколишнього середовища, такі як температура, напруга, старіння та шуми. Ці варіації можуть призвести до неузгодженості у створенні ключів та автентифікації.

2. Через чутливість до факторів навколишнього середовища ФНФ можуть з часом виявляти проблеми зі стабільністю та надійністю. Варіації, які спочатку вважалися випадковими, можуть стати більш передбачуваними з віком пристрою.
3. Кваліфіковані зловмисники можуть спробувати створити моделі, які передбачають поведінку ФНФ на основі підмножини вимірювань. У разі успіху це може поставити під загрозу безпеку ключів, згенерованих ФНФ.
4. ФНФ часто вимагають калібрування, щоб зменшити неточності та помилки. Це вносить додаткову складність, а сам процес калібрування може стати мішенню для атак.
5. Довжина ключів, згенерованих ФНФ, часто обмежена фізичними характеристиками пристрою.
6. Різні реалізації ФНФ можуть мати різні характеристики та рівні безпеки, що створює проблеми взаємодії та стандартизації.

Підсумовуючи, фізично не клоновані функції пропонують унікальний підхід до генерації безпечних криптографічних ключів і автентифікації пристроїв. Однак вони мають проблеми, пов’язані зі стабільністю, варіаціями навколишнього середовища, моделюванням атак і калібруванням.

Біометрична автентифікація

Біометрична автентифікація — це метод безпеки, який використовує унікальні фізичні чи поведінкові особи або певні фізичні характеристики пристрою для їх підтвердження. Він пропонує більш безпечну та зручну альтернативу традиційним методам, таким як паролі чи PIN-коди. Системи біометричної автентифікації фіксують і аналізують ці унікальні характеристики, щоб надати доступ до пристроїв, систем або послуг.

Переваги:

1. Кожен мікроконтролер має свої унікальні фізичні характеристики, які можуть бути використані для ідентифікації пристрою. Це забезпечує високий рівень безпеки, оскільки кожен пристрій може бути однозначно ідентифікований.
2. Біометричні характеристики пристрою складніше підробити або скопіювати, порівняно зі звичайними паролями або кодами доступу. Це забезпечує високий рівень захисту від несанкціонованого доступу.
3. Використання біометричних методів автентифікації може бути більш зручним для користувачів, оскільки вони не потребують запам’ятовування паролів або інших ідентифікаторів.

Недоліки:

1. Збір та зберігання біометричних даних може викликати проблеми з конфіденційністю, оскільки ця інформація є дуже особистою. Несанкціонований доступ до біометричних даних може мати серйозні наслідки для безпеки користувачів.
2. Біометричні системи можуть бути вразливі до різних атак, таких як підробка або перехоплення біометричних даних. Недоліки системи можуть використовувати для отримання несанкціонованого доступу до пристроїв чи систем.
3. Деякі біометричні методи можуть мати технічні обмеження, такі як проблеми з точністю або швидкістю ідентифікації. В цих випадках

користувачам може знадобитися додатковий час або зусилля для успішної автентифікації.

Підсумовуючи, біометрична автентифікація забезпечує підвищену безпеку та зручність, але пов'язана з проблемами конфіденційності, захистом даних, точністю та потенційною вразливістю. Організації повинні ретельно оцінити ризики та переваги, та впровадити відповідні запобіжні заходи для усунення потенційних недоліків біометричних систем автентифікації.

Автентифікація на основі пароля

Автентифікація за паролем є одним із найпоширеніших і широко використовуваних методів перевірки ідентичності користувачів, які отримують доступ до цифрових систем, облікових записів або ресурсів. Користувачі вводять секретну парольну фразу або комбінацію символів, відому як пароль, щоб підтвердити свою особу.

Переваги

1. Паролі зрозумілі та знайомі користувачам, оскільки протягом тривалого часу вони були поширеним методом автентифікації.
2. Впровадження автентифікації на основі пароля є відносно дешевим у порівнянні з деякими іншими методами автентифікації, які вимагають спеціалізованого обладнання чи інфраструктури.
3. Користувачі можуть легко вводити паролі на різних пристроях, що робить автентифікацію на основі пароля зручною для широкого кола сценаріїв.
4. Автентифікація на основі пароля працює практично на всіх пристроях і платформах, забезпечуючи широку сумісність.
5. Користувачі можуть змінити свої паролі в будь-який час, забезпечуючи гнучкість для оновлень або у разі підозри на порушення безпеки.
6. Паролі не залежать від зовнішніх пристроїв або каналів зв'язку, що робить їх доступними в різних ситуаціях.

Недоліки

1. Паролі можуть бути вразливими до різноманітних атак, таких як атаки грубою силою, атаки за словником і використання слабких паролів або паролі, які легко вгадати.
2. Користувачі часто повторно використовують паролі для кількох служб, що збільшує ризик злому та несанкціонованого доступу, якщо одна служба скомпрометована.
3. Паролі чутливі до фішингових атак, коли зловмисники обманом змушують користувачів розкрити їхні паролі. Атаки соціальної інженерії також можуть маніпулювати користувачами, щоб вони відмовилися від своїх паролів.
4. Користувачам потрібно запам'ятовувати кілька паролів, що призводить потенційно небезпечних практик, таких як запис та зберігання паролів в не захищених місцях.
5. Для підвищення безпеки складні вимоги до пароля (наприклад, цифри, спеціальні символи, великі та малі літери) можуть призвести до труднощів із запам'ятовуванням паролів.
6. Повторні невдалі спроби входу можуть призвести до тимчасового або постійного блокування облікового запису, що створює незручності для користувачів і може бути використано зловмисниками.

7. Паролі часто прив’язані до конкретних облікових записів користувачів, що означає, що анонімність не гарантується при використанні автентифікації на основі пароля.
8. Зловмисники можуть побачити або записати пароль користувача, який його вводить, що загрожує безпеці.
9. Якщо пристрій користувача заражено кейлогерами або зловмисним програмним забезпеченням, паролі можуть бути захоплені під час їх введення.

Підсумовуючи, можна сказати, що автентифікація на основі пароля пропонує звичність і легкість у використанні, але пов’язана з проблемами безпеки, особливо в контексті слабких паролів, повторного використання пароля та вразливості до фішингових атак.

В табл. 1 наведено порівняння описаних методів на вразливості до найпоширеніших атак на автентифікацію. Висновок полягає в тому, що не існує ідеального та універсального методу автентифікації мікроконтролерів, який би відповідав усім вимогам без винятків. Кожен метод має свої переваги та недоліки, ідеальний лише у своїй специфічній області застосування. Тому для забезпечення високого рівня безпеки автентифікації мікроконтролерів рекомендується комбінувати та використовувати вже існуючі методи за ідеальних умов.

Наприклад, можна поєднувати парольні дані з фізично не клонованими функціями для створення багатофакторної автентифікації, яка посилює безпеку системи. При цьому важливо враховувати особливості кожного методу та їхню придатність для конкретного застосування.

Більше того, необхідно уважно аналізувати ймовірні загрози та ризики, які можуть виникнути в контексті конкретного застосування мікроконтролерів, і вибирати відповідні методи автентифікації з урахуванням цих факторів. Такий підхід дозволить підвищити ефективність заходів безпеки та мінімізувати можливі ризики використання мікроконтролерів у системах та пристроях.

Таблиця 1

Порівняльна характеристика методів автентифікації за можливими атаками

Назва атаки	**Метод автентифікації**		
	Парольна автентифікація	**Біометрична автентифікація**	**Фізично не клоновані функції**
Brute force attack	Піддається	Не піддається	Піддається
Phishing	Піддається	Піддається	Піддається
Social engineering	Піддається	Піддається	Піддається
SQL injection	Піддається	Не піддається	Не піддається
Attacks on two-factor authentication	Піддається	Не піддається	Не піддається
Attacks on weakly protected Wi-Fi networks	Піддається	За певних умов піддається	За певних умов піддається
Password interception attacks	Піддається	За певних умов піддається	За певних умов піддається
"The Man In the middle"	Піддається	За певних умов піддається	За певних умов піддається
Identity attacks	Піддається	Піддається	Не піддається
Session hijacking attacks	Піддається	Не піддається	Не піддається

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Підсумовуючи, безпека сучасних мікроконтролерів має першочергове значення для забезпечення цілісності, конфіденційності та доступності систем, які вони забезпечують. Оскільки ці мініатюрні комп'ютерні пристрої стають все більш поширеними в різних галузях промисловості та застосуваннях, усунення вразливостей у їхній безпеці стає невідкладною задачею. Однак саме розмаїття архітектур мікроконтролерів, додатків і варіантів використання становить величезну проблему для розробки комплексних рішень безпеки.

Очевидно, що універсальний підхід до захисту мікроконтролерів не є ані практичним, ані здійсненним. Кожен тип мікроконтролера може мати унікальні функції, інтерфейси та вразливості, які вимагають індивідуальних заходів безпеки. Однак складність і поширення систем на основі мікроконтролерів підкреслюють важливість пошуку уніфікованого, але адаптованого рішення, яке може вмістити різноманітний ландшафт мікроконтролерів, одночасно забезпечуючи надійний захист від поширених загроз.

Зусилля щодо покращення безпеки мікроконтролерів повинні надавати пріоритет співпраці між зацікавленими сторонами галузі, дослідниками та регуляторними органами для розробки стандартизованих інфраструктур безпеки, передового досвіду та схем сертифікації. Крім того, прогрес у технологіях безпеки, таких як апаратні модулі безпеки, безпечні механізми завантаження та довірені середовища виконання обіцяють підвищити стійкість вбудованих систем на основі мікроконтролерів проти нових кіберзагроз.

Крім того, розробка відкритих стандартів і сумісних протоколів безпеки може сприяти бездоганній інтеграції та сумісності між різними платформами мікроконтролерів, одночасно забезпечуючи сумісність із існуючими та новими технологіями безпеки. Розвиваючи культуру прозорості, підзвітності та постійного вдосконалення, зацікавлені сторони можуть колективно вирішувати проблеми безпеки, властиві сучасним мікроконтролерам, і зберігати довіру та впевненість користувачів у цих критично важливих компонентах нашого взаємопов'язаного світу.

По суті, пошук унікального та загального вирішення проблем безпеки, які створюють сучасні мікроконтролери, вимагає узгоджених зусиль, щоб збалансувати гнучкість, масштабованість та ефективність. Застосовуючи цілісний підхід до безпеки мікроконтролерів, який наголошує на співпраці, інноваціях і адаптивності, ми можемо зменшити ризики, зміцнити захист і прокласти шлях для більш безпечної та стійкої цифрової екосистеми на основі технології мікроконтролерів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kleber, S. (2015). Secure Execution Architecture based on PUF-driven Instruction Level Code Encryption: preprint. *Cryptology ePrint Archive*.
2. Khalil, D. (2019). A Comparison Survey Study on RFID Based Anti-Counterfeiting Systems. *J. Sens. Actuator Netw. 8(3),* 37. https://doi.org/10.3390/jsan8030037
3. Karimian, N. (2019). *DRAMNet: Authentication based on Physical Unique Features of DRAM Using Deep Convolutional Neural Networks.* https://doi.org/10.48550/arXiv.1902.09094
4. Yang, D. (2019). Security and Accuracy of Fingerprint-Based Biometrics: A Review. *Symmetry, 11(2),* 141. https://doi.org/10.3390/sym11020141

5. Shamsoshoara, A., Korenda, A., Fatemeh, A., & Sherali, Z. (2020). A survey on physical unclonable function (PUF)-based security solutions for Internet of Things. *Comp. Netw. 183*. https://doi.org/10.1016/j.comnet.2020.107593
6. Nadimi Goki, P., Civelli, S., Parente, E. (2023). *Optical identification using physical unclonable functions*. https://doi.org/10.48550/arXiv.2305.02141
7. Shamala, L., Zayaraz, D., Vivekanandan, D. (2021). Lightweight Cryptography Algorithms for Internet of Things enabled Networks: An Overview. *Journal of Physics: Conference Series, 1717.* https://doi.org/10.1088/1742-6596/1717/1/012072
8. van de Meent, T. A. (2022). *Comparative Study on Lightweight Authentication Protocols in IoT context*. https://essay.utwente.nl/89452/1/van_de_Meent_BA_EEMCS.pdf.
9. Papathanasaki, M. (2022). Modern Authentication Methods: A Comprehensive Survey. *AI, Computer Science and Robotics Technology*. https://doi.org/10.5772/acrt.08
10. Yang, A. (2022). A Lightweight and Practical Anonymous Authentication Protocol Based on Bit-Self-Test PUF. *Electronics, 11(5),* 772. https://doi.org/10.3390/electronics11050772
11. Meixner, A. (2023). *Fingerprinting Chips For Traceability.* https://semiengineering.com/fingerprinting-chips-for-traceability/
12. Mahadeen, M. (2023). Smartphone User Identification/Authentication Using Accelerometer and Gyroscope Data. *Sustainability, 15(13),* 10456. https://doi.org/10.3390/su151310456
13. Gupta, C. (2024). *A Lightweight and Secure PUF-Based Authentication and Key-exchange Protocol for IoT Devices.* https://doi.org/10.21203/rs.3.rs-3850019/v1
14. Xi, D. (2024). Device Identity Recognition Based on an Adaptive Environment for Intrinsic Security Fingerprints. *Electronics, 13(3),* 656. https://doi.org/10.3390/electronics13030656
15. Nie, S., Liu, L., & Du, Y., (2017). *Free-fall: Hacking tesla from wireless to can bus*.
16. Gassend, B., Clarke, D., van Dijk, M., & Devadas, S., (2002). Silicon physical random functions, *Proceedings of the 9th ACM Conference on Computer and Communications Security,* 148–160. https://doi.org/10.1145/586110.586132
17. Anagnostopoulos, N. A., Katzenbeisser, S., Chandy, J., & Tehranipoor, F., (2018). An overview of dram-based security primitives. *Cryptography, 2(2).*
18. Tehranipoor, F., Karimian, N., Yan, W., & Chandy, J. A., (2017). Dram-based intrinsic physically unclonable functions for system-level security and authentication. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 25*, 1085–1097.
19. Tehranipoor, F., Yan, W., & Chandy, J. A. (2016). Robust hardware true random number generators using dram remanence effects. *IEEE International Symposium on Hardware Oriented Security and Trust (HOST),* 79–84.
20. Schaller, A., Xiong, W., Anagnostopoulos, N. A., Saleem, M. U., Gabmeyer, S., Skoric, B., Katzenbeisser, S., & Szefer, J., (2018). Decay-based dram pufs in commodity devices. *IEEE Transactions on Dependable and Secure Computing.*
21. Talukder, B. M. S. B., Ray, B., Tehranipoor, M., Forte, D., & Rahman, M. T. (2018). LDPUF: exploiting DRAM latency variations to generate robust device signatures. arXiv preprint. https://doi.org/10.48550/arXiv.1808.02584
22. Kim, J. S., Patel, M., Hassan, H., & Mutlu, O. (2018). The dram latency puf: Quickly evaluating physical unclonable functions by exploiting the latency-reliability tradeoff in modern commodity dram devices. *IEEE International Symposium on High Performance Computer Architecture (HPCA),* 194–207.
23. Anagnostopoulos, N. A., Arul, T., Fan, Y., Hatzfeld, C., Schaller, A., Xiong, W., Jain, M., Saleem, M. U., Lotichius, J., Gabmeyer, S., Szefer, J., & Katzenbeisser, S. (2018). Intrinsic run-time row hammer pufs: Leveraging the row hammer effect for run-time cryptography and improved security. *Cryptography, 2(3).*
24. Ruhrmair, U., Sehnke, F., Zolter, J. S., Dror, G., Devadas, S., & Schmidhuber, J. (2010). Modeling attacks on physical unclonable functions. *Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS '10,* 237–249.
25. Rhrmair, U., Slter, J., Sehnke, F., Xu, X., Mahmoud, A., Stoyanova, V., Dror, G., Schmidhuber, J., Burleson, W., & Devadas, S., (2013). Puf modeling attacks on simulated and silicon data. *IEEE Transactions on Information Forensics and Security, 8,* 1876–1891.
26. Ganji, F., Tajik, S., Faßler, F., & Seifert, J.-P. (2016). Strong machine learning attack against pufs with no mathematical model. *Cryptographic Hardware and Embedded Systems – CHES 2016,* 391–411.
27. Herder, C., Yu, M., Koushanfar, F., & Devadas, S. (2014). Physical unclonable functions and applications: A tutorial. *Proceedings of the IEEE, 102,* 1126–1141.

28. Yu, M.-D. M., M'Raihi, D., Sowell, R., & Devadas, S. (2011). Lightweight and secure puf key storage using limits of machine learning. *Cryptographic Hardware and Embedded Systems – CHES 2011*, 358–373.
29. Paral, Z., & Devadas, S., (2011). Reliable and efficient puf-based key generation using pattern matching. *IEEE International Symposium on Hardware-Oriented Security and Trust*, 128–133.
30. Addabbo, T., Fort, A., Marco, M. D., Pancioni, L., Vignoli, V., (2013). Physically unclonable functions derived from cellular neural networks. *IEEE Transactions on Circuits and Systems I: Regular Papers, 60*, 3205–3214.
31. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. *MIT Press.*
32. Tehranipoor, F., Karimian, N., Yan, W., & Chandy, J. A. (2017). Investigation of dram pufs reliability under device accelerated aging effects. *IEEE International Symposium on Circuits and Systems (ISCAS)*, 1–4.
33. Srivastava, N., Hinton, G., Krizhevsky, A., Sutskever, I., & Salakhutdinov, R. (2014). Dropout: A simple way to prevent neural networks from overfitting. *Journal of Machine Learning Research, 15*, 1929–1958.
34. Kushner, H. J., & Yin, G. G. (2003). Stochastic Approximation and Recursive Algorithms and Applications. *Stochastic Modelling and Applied Probability. Springer Science & Business Media*, *35*.
35. Kingma, D. P., Ba, J. (2014). Adam: A method for stochastic optimization. arXiv preprint. https://doi.org/10.48550/arXiv.1412.6980
36. Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). Imagenet classification with deep convolutional neural networks. *Proceedings of the 25th International Conference on Neural Information Processing Systems, 1*, 1097–1105.
37. Simonyan, K., & Zisserman, A. (2014). *Very deep convolutional networks for large-scale image recognition.* arXiv preprint. https://doi.org/10.48550/arXiv.1409.1556

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023

Taras Chura
Graduate student of the Department of Security of Information Technologies
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0009-0001-1898-9879
taras.r.chura@lpnu.ua

Nazar Chura
Graduate student of the Department of Security of Information Technologies
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0009-0006-9072-0045
nazar.r.chura@lpnu.ua

OVERVIEW OF MODERN AUTHENTICATION METHODS FOR MICROCONTROLLERS

Abstract. The paper is devoted to the study of modern authentication methods for microcontrollers, which play a crucial role in today's technological landscape. Microcontrollers serve as the foundation for most embedded devices used in various sectors, including consumer electronics, automotive systems, industrial equipment, and medical devices. They perform essential functions related to the control, monitoring, and management of numerous processes and systems. Given the widespread adoption of microcontrollers in critical infrastructures, ensuring their security has become a top priority. Authentication of microcontrollers is vital for preventing unauthorized access and cyberattacks, which could lead to serious consequences such as data breaches, system control, or failures in critical services. The paper examines the significance of microcontroller security in modern technologies and explores the potential risks arising from the use of unsecured microcontrollers. It also analyzes the state-of-the-art authentication methods used to protect microcontrollers. Special attention is given to comparing different approaches to authentication, which include both traditional and novel methods based on cryptography, physically unclonable functions (PUF), and biometrics. For each method, the paper outlines its advantages, disadvantages, and application areas, along with an assessment of their effectiveness in various security scenarios. Furthermore, the paper presents the results of practical implementation of some authentication methods in real-world examples, which demonstrate their viability and effectiveness in securing modern systems. The authors also suggest future research directions in this field, particularly the development of new authentication methods that combine high reliability with ease of implementation in the context of rapidly evolving technologies and cyber threats.

Keywords: cyber security; vulnerabilities; microcontrollers; authentication of microcontrollers.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Kleber, S. (2015). Secure Execution Architecture based on PUF-driven Instruction Level Code Encryption: preprint. *Cryptology ePrint Archive*.
2. Khalil, D. (2019). A Comparison Survey Study on RFID Based Anti-Counterfeiting Systems. *J. Sens. Actuator Netw. 8(3),* 37. https://doi.org/10.3390/jsan8030037
3. Karimian, N. (2019). *DRAMNet: Authentication based on Physical Unique Features of DRAM Using Deep Convolutional Neural Networks.* https://doi.org/10.48550/arXiv.1902.09094
4. Yang, D. (2019). Security and Accuracy of Fingerprint-Based Biometrics: A Review. *Symmetry, 11(2),* 141. https://doi.org/10.3390/sym11020141
5. Shamsoshoara, A., Korenda, A., Fatemeh, A., & Sherali, Z. (2020). A survey on physical unclonable function (PUF)-based security solutions for Internet of Things. *Comp. Netw. 183*. https://doi.org/10.1016/j.comnet.2020.107593
6. Nadimi Goki, P., Civelli, S., Parente, E. (2023). *Optical identification using physical unclonable functions*. https://doi.org/10.48550/arXiv.2305.02141

7. Shamala, L., Zayaraz, D., Vivekanandan, D. (2021). Lightweight Cryptography Algorithms for Internet of Things enabled Networks: An Overview. *Journal of Physics: Conference Series, 1717.* https://doi.org/10.1088/1742-6596/1717/1/012072
8. van de Meent, T. A. (2022). *Comparative Study on Lightweight Authentication Protocols in IoT context*. https://essay.utwente.nl/89452/1/van_de_Meent_BA_EEMCS.pdf.
9. Papathanasaki, M. (2022). Modern Authentication Methods: A Comprehensive Survey. *AI, Computer Science and Robotics Technology*. https://doi.org/10.5772/acrt.08
10. Yang, A. (2022). A Lightweight and Practical Anonymous Authentication Protocol Based on Bit-Self-Test PUF. *Electronics, 11(5),* 772. https://doi.org/10.3390/electronics11050772
11. Meixner, A. (2023). *Fingerprinting Chips For Traceability.* https://semiengineering.com/fingerprinting-chips-for-traceability/
12. Mahadeen, M. (2023). Smartphone User Identification/Authentication Using Accelerometer and Gyroscope Data. *Sustainability, 15(13),* 10456. https://doi.org/10.3390/su151310456
13. Gupta, C. (2024). *A Lightweight and Secure PUF-Based Authentication and Key-exchange Protocol for IoT Devices.* https://doi.org/10.21203/rs.3.rs-3850019/v1
14. Xi, D. (2024). Device Identity Recognition Based on an Adaptive Environment for Intrinsic Security Fingerprints. *Electronics, 13(3),* 656. https://doi.org/10.3390/electronics13030656
15. Nie, S., Liu, L., & Du, Y., (2017). *Free-fall: Hacking tesla from wireless to can bus*.
16. Gassend, B., Clarke, D., van Dijk, M., & Devadas, S., (2002). Silicon physical random functions, *Proceedings of the 9th ACM Conference on Computer and Communications Security,* 148–160. https://doi.org/10.1145/586110.586132
17. Anagnostopoulos, N. A., Katzenbeisser, S., Chandy, J., & Tehranipoor, F., (2018). An overview of dram-based security primitives. *Cryptography, 2(2).*
18. Tehranipoor, F., Karimian, N., Yan, W., & Chandy, J. A., (2017). Dram-based intrinsic physically unclonable functions for system-level security and authentication. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 25*, 1085–1097.
19. Tehranipoor, F., Yan, W., & Chandy, J. A. (2016). Robust hardware true random number generators using dram remanence effects. *IEEE International Symposium on Hardware Oriented Security and Trust (HOST),* 79–84.
20. Schaller, A., Xiong, W., Anagnostopoulos, N. A., Saleem, M. U., Gabmeyer, S., Skoric, B., Katzenbeisser, S., & Szefer, J., (2018). Decay-based dram pufs in commodity devices. *IEEE Transactions on Dependable and Secure Computing.*
21. Talukder, B. M. S. B., Ray, B., Tehranipoor, M., Forte, D., & Rahman, M. T. (2018). LDPUF: exploiting DRAM latency variations to generate robust device signatures. arXiv preprint. https://doi.org/10.48550/arXiv.1808.02584
22. Kim, J. S., Patel, M., Hassan, H., & Mutlu, O. (2018). The dram latency puf: Quickly evaluating physical unclonable functions by exploiting the latency-reliability tradeoff in modern commodity dram devices. *IEEE International Symposium on High Performance Computer Architecture (HPCA),* 194–207.
23. Anagnostopoulos, N. A., Arul, T., Fan, Y., Hatzfeld, C., Schaller, A., Xiong, W., Jain, M., Saleem, M. U., Lotichius, J., Gabmeyer, S., Szefer, J., & Katzenbeisser, S. (2018). Intrinsic run-time row hammer pufs: Leveraging the row hammer effect for run-time cryptography and improved security. *Cryptography, 2(3).*
24. Ruhrmair, U., Sehnke, F., Zolter, J. S., Dror, G., Devadas, S., & Schmidhuber, J. (2010). Modeling attacks on physical unclonable functions. *Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS '10,* 237–249.
25. Rhrmair, U., Slter, J., Sehnke, F., Xu, X., Mahmoud, A., Stoyanova, V., Dror, G., Schmidhuber, J., Burleson, W., & Devadas, S., (2013). Puf modeling attacks on simulated and silicon data. *IEEE Transactions on Information Forensics and Security, 8,* 1876–1891.
26. Ganji, F., Tajik, S., Faßler, F., & Seifert, J.-P. (2016). Strong machine learning attack against pufs with no mathematical model. *Cryptographic Hardware and Embedded Systems – CHES 2016,* 391–411.
27. Herder, C., Yu, M., Koushanfar, F., & Devadas, S. (2014). Physical unclonable functions and applications: A tutorial. *Proceedings of the IEEE, 102*, 1126–1141.
28. Yu, M.-D. M., M'Raihi, D., Sowell, R., & Devadas, S. (2011). Lightweight and secure puf key storage using limits of machine learning. *Cryptographic Hardware and Embedded Systems – CHES 2011*, 358–373.
29. Paral, Z., & Devadas, S., (2011). Reliable and efficient puf-based key generation using pattern matching. *IEEE International Symposium on Hardware-Oriented Security and Trust,* 128–133.

30. Addabbo, T., Fort, A., Marco, M. D., Pancioni, L., Vignoli, V., (2013). Physically unclonable functions derived from cellular neural networks. *IEEE Transactions on Circuits and Systems I: Regular Papers, 60*, 3205–3214.
31. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. *MIT Press.*
32. Tehranipoor, F., Karimian, N., Yan, W., & Chandy, J. A. (2017). Investigation of dram pufs reliability under device accelerated aging effects. *IEEE International Symposium on Circuits and Systems (ISCAS)*, 1–4.
33. Srivastava, N., Hinton, G., Krizhevsky, A., Sutskever, I., & Salakhutdinov, R. (2014). Dropout: A simple way to prevent neural networks from overfitting. *Journal of Machine Learning Research, 15*, 1929–1958.
34. Kushner, H. J., & Yin, G. G. (2003). Stochastic Approximation and Recursive Algorithms and Applications. *Stochastic Modelling and Applied Probability. Springer Science & Business Media*, *35*.
35. Kingma, D. P., Ba, J. (2014). Adam: A method for stochastic optimization. arXiv preprint. https://doi.org/10.48550/arXiv.1412.6980
36. Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). Imagenet classification with deep convolutional neural networks. *Proceedings of the 25th International Conference on Neural Information Processing Systems, 1*, 1097–1105.
37. Simonyan, K., & Zisserman, A. (2014). *Very deep convolutional networks for large-scale image recognition.* arXiv preprint. https://doi.org/10.48550/arXiv.1409.1556